



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/772,433	02/06/2004	Marcus Leech	57983.000164	5978
7590	10/19/2007		EXAMINER	
Thomas E. Anderson Hunton & Williams LLP 1900 K Street, N.W. Washington, DC 20006-1109			LANIER, BENJAMIN E	
			ART UNIT	PAPER NUMBER
			2132	
			MAIL DATE	DELIVERY MODE
			10/19/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)
	10/772,433	LEECH, MARCUS
	Examiner	Art Unit
	Benjamin E. Lanier	2132

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) Responsive to communication(s) filed on 12 September 2007.
- 2a) This action is FINAL. 2b) This action is non-final.
- 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) Claim(s) 1-20 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) Claim(s) _____ is/are allowed.
- 6) Claim(s) 1-20 is/are rejected.
- 7) Claim(s) _____ is/are objected to.
- 8) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) The specification is objected to by the Examiner.
- 10) The drawing(s) filed on _____ is/are: a) accepted or b) objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) All b) Some * c) None of:
 1. Certified copies of the priority documents have been received.
 2. Certified copies of the priority documents have been received in Application No. _____.
 3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date: _____ |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| Paper No(s)/Mail Date: _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

Response to Amendment

1. Applicant's amendment filed 12 September 2007 amends claims 1-5, 7, 8, 1, 11, 13-15, 19, and 20. Applicant's amendment has been fully considered and entered.

Response to Arguments

2. Applicant argues, "that the first mask value and the second mask value as recited in claim 1 are not equivalent values...however, that, in certain circumstances (e.g. when computed to be the same based upon the computation factors as set forth in claims 2 and 7), the first mask value and the second mask value may have the same value." Based on this admission by Applicant, the current rejection of claim 1 is hereby maintained since the two claimed mask values can indeed have the same value, which is shown in Rogaway (Figure 1).

3. Applicant argues, "Rogaway discloses applying an identical offset $Z[i]$ to all but one string of a message M before and after a block cipher E_k (see pages 4-6)." This argument is not persuasive because the encryption process of Rogaway does not use an identical offset Z for all but one string, but instead uses a different offset for each message block in the encryption process (See Figure 1). Figure 1 of Rogaway shows that the encryption of message block 1 utilizes offset $Z[1]$, while the encryption of message block 2 utilizes offset $Z[2]$, and so on.

4. Applicant argues, "Rogaway fails to disclose or even suggest the elements of applying a XOR function to all blocks of a message to compute a XOR-sum, applying a first mask value to the XOR-sum, encrypting the masked XOR-sum using a block cipher and a first key, and applying a second mask value to the encrypted XOR-sum to generate an integrity tag, as claimed." This argument is not persuasive because Rogaway discloses that each message blocks

is concatenated (Page 5, checksum generation function), which meets the limitation of applying a XOR function to all message blocks of a message to compute a XOR-sum. The checksum is then XOR'd with Z[m] (Page 5, calculation of value 'T'), which meets the limitation of applying a third mask value to the XOR-sum. The result of the XOR function is then encrypted (Page 5, calculation of value 'T'), which meets the limitation of encrypting the masked XOR-sum using the block cipher and the first key. Rogaway does not disclose XOR'ing the result of the encryption with a value. However, it would have been obvious to one of ordinary skill in the art at the time the invention was made to XOR the data after the block algorithm, in addition to before, because this technique is not susceptible to meet-in-the-middle attack as taught by Schneier (Page 367).

5. Applicant argues, "Rogaway also discloses applying a string L and an offset Z[m] to one string of a message M before a block cipher Ek, as well as applying the same message string M[m] after the block cipher Ek (see pages 4-6)." Applicant has not considered the proposed modification of Rogaway used to rejection claim 12, which suggests that it would have been obvious to one of ordinary skill in the art at the time the invention was made to XOR the data after the block algorithm, in addition to before, because this technique is not susceptible to meet-in-the-middle attack as taught by Schneier (Page 367).

6. Applicant argues, "Rogaway also discloses applying and limiting as described above to a checksum of xor'ed message strings M, ciphertext string C[m], and block ciphered string Y[m]." Applicant appears to have not considered the entire rejection, as mentioned above. Rogaway teaches applying a XOR function to all blocks of a message to compute a XOR-sum (See page 5, calculation of Checksum), applying a first mask value to the XOR-sum (See page 5, Checksum

Art Unit: 2132

$\oplus Z[m])$, encrypting the masked XOR-sum using a block cipher and a first key (See page 5, $E_k(\text{Checksum} \oplus Z[m])$). Rogaway does not disclose XOR'ing the result of the encryption with a value. However, it would have been obvious to one of ordinary skill in the art at the time the invention was made to XOR the data after the block algorithm, in addition to before, because this technique is not susceptible to meet-in-the-middle attack as taught by Schneier (Page 367).

7. Applicant argues, "Regarding combining Schneier with Rogaway to arrive at the claimed invention, such a combination would result in an inoperable methodology since replacing the limiting of Rogaway with an additional xor function as mentioned by Schneier would not result in a limited tag length τ , which is required by Rogaway." This argument is not persuasive because the proposed modification of Rogaway never alleged "replacing the limiting of Rogaway with an additional xor function" as alleged by Applicant, but instead suggested exclusive or'ing the result of encrypting ($\text{Checksum} \oplus Z[m])$. Additionally, Applicant's allegation of inoperability is unsupported by any actual cited evidence and is therefore unpersuasive.

8. Applicant's argument that the amendments to claims 10 and 19 have overcome the previous §101 rejections has been fully considered and is persuasive. The previous §101 rejections of claims 10 and 19 have been withdrawn.

9. Applicant's arguments with respect to the previous §112 rejections of claims 2, 7, 13, and 17, have been fully considered and are persuasive. The previous §112 rejections of claims 2, 7, 13, and 17 have been withdrawn.

Art Unit: 2132

10. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

11. Claims 1, 8, 9, 11 are rejected under 35 U.S.C. 102(b) as being anticipated by Rogaway, OCB: A Block-Cipher Mode of Operation for Efficient Authenticated Encryption (from IDS dated 06 February 2004). Referring to claims 1, 11, Rogaway discloses encrypting a message by exclusive or'ing a block of the message with a corresponding block of a generated value (Page 5, $M[i] \oplus Z[i]$), which meets the limitation of whitening at least one message block with a first mask value. The result of that exclusive or operation is encrypted (Page 5) using a block cipher (Page 4), which meets the limitation of encrypting the at least one whitened message block using a block cipher and a first key. The result of the encryption is the exclusive or'ed with a corresponding block of the generated value (Page 5), which meets the limitation of whitening the at least one encrypted message block with a second mask value to generate at least one corresponding output ciphertext block.

Referring to claim 8, Rogaway describes the decryption process where cipherblocks are XOR'd with the corresponding block of the generated Z value (Page 5), which meets the limitation of whitening the at least one output ciphertext block with the second mask value. The result of the XOR function is decrypted with the key (Page 5), which meets the limitaiton of decrypting the at least one whitening ciphertext block using a block cipher and the first key. The decrypted value is then XOR's with the corresponding block of the generated Z value (Page 5),

which meets the limitation of whitening the at least one decrypted block with a first mask value to generate at least one corresponding message block.

Referring to claim 9, Rogaway discloses that the block cipher used is the AES block cipher (Page 6, first paragraph), which meets the limitation of the block cipher is AES.

Claim Rejections - 35 USC § 103

12. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

13. The factual inquiries set forth in *Graham v. John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

14. Claims 2-7, 10, 12-20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Rogaway, in view of Schneier. Referring to claim 2, Rogaway discloses that the corresponding block of the generated value is generated based on the XOR of an encrypted nonce (Page 5, R) and an encrypted value (Page 5, L), which meets the limitaiton of the first mask value is computed by applying a XOR function to a first value derived from a nonce value and a second value derived from encrypting a third value using the block cipher and a key, wherein the second mask value is computed by applying a XOR function to a fourth value derived from the nonce

Art Unit: 2132

value and a fifth value derived from encrypting a sixth value using the block cipher and a key since by Applicant's own admission (Remarks page 12, end of first paragraph) "the first mask value and the second mask value may have the same value", which would require the corresponding values above to be identical. Rogaway does not specify that the key used to encrypt the value to generate the 'L' (Page 5) is different than the key used to encrypt $M[i] \oplus Z[i]$ (Page 5). However, it would have been obvious to one of ordinary skill in the art at the time the invention was made to use multiple keys in the encryption algorithm in order to enhance the strength of the encryption algorithm by making the algorithm more difficult to break. Using only a single encryption key is easier break than using mutliple because an attacker would only need to discover the one key as opposed to having to discover every key that is used in the encryption algorithm. Rogaway also does not disclose applying a substitution function to the result of the XOR function on L and R. However, it would have been obvious to one of ordinary skill in the art at the time the invention was made to perform a subsititution function on the result of the XOR function on L and R because substitution operations are an important part of block cipher algorithms that give them security as taught by Schneier (Page 275).

Referring to claim 3, Rogaway discloses that to compute the R value, the nonce is XOR'd with L and the result of the XOR function is encrypted with key K (Page 5), which meets the limitation of the first and fourth values derived from the nonce value are permutations of a binary value computed by encrypting the nonce value using the block cipher and the first key.

Referring to claim 4, Rogaway discloses that the L value is generated by encrypted a finite string (Page 5), but does not disclose that the finite string is randomly generated. It would have been obvious to one of ordinary skill in the art at the time the invention was made to

Art Unit: 2132

randomly generated the finite string used to calculate the L value in Rogaway such that the finite string would be unpredictable, thus increasing the security of cryptographic algorithm as taught by Schneier (Page 45).

Referring to claim 5, Rogaway discloses encrypting a message by exclusive or'ing a block of the message with a corresponding block of a generated value (Page 5, $M[i] \oplus Z[i]$). The result of that exclusive or operation is encrypted (Page 5) using a block cipher (Page 4). The result of the encryption is the exclusive or'ed with a corresponding block of the generated value (Page 5), which meets the limitation of the steps of whitening each comprise the step of applying a XOR function.

Referring to claims 6, 12, 20, Rogaway discloses that each message blocks is concatenated (Page 5, checksum generation function), which meets the limitation of applying a XOR function to all message blocks of a message to compute a XOR-sum. The checksum is then XOR'd with $Z[m]$ (Page 5, calculation of value 'T'), which meets the limitation of applying a third mask value to the XOR-sum. The result of the XOR function is then encrypted (Page 5, calculation of value 'T'), which meets the limitation of encrypting the masked XOR-sum using the block cipher and the first key. Rogaway does not disclose XOR'ing the result of the encryption with a value. However, it would have been obvious to one of ordinary skill in the art at the time the invention was made to XOR the data after the block algorithm, in addition to before, because this technique is not susceptible to meet-in-the-middle attack as taught by Schneier (Page 367).

Referring to claims 7, 13, Rogaway discloses that the corresponding block of the generated value is generated based on the XOR of an encrypted nonce (Page 5, R) and an

Art Unit: 2132

encrypted value (Page 5, L), which meets the limitaiton of the first/third mask value is computed by applying a XOR function to a first value derived from a nonce value and a second value derived from encrypting a third value using the block cipher and a key, wherein the second/fourth mask value is computed by applying a XOR function to a fourth value derived from the nonce value and a fifth value derived from encrypting a sixth value using the block cipher and a key. Rogaway does not specify that the key used to encrypt the value to generate the 'L' (Page 5) is different than the key used to encrypt $M[i] \oplus Z[i]$ (Page 5). However, it would have been obvious to one of ordinary skill in the art at the time the invention was made to use multiple keys in the encryption algorithm in order to enhance the strength of the encryption algorithm by making the algorithm more difficult to break. Using only a single encryption key is easier break than using mutliple because an attacker would only need to discover the one key as opposed to having to discover every key that is used in the encryption algorithm. Rogaway also does not disclose applying a substitution function to the result of the XOR function on L and R. However, it would have been obvious to one of ordinary skill in the art at the time the invention was made to perform a subsititution function on the result of the XOR function on L and R because substitution operations are an important part of block cipher algorithms that give them security as taught by Schneier (Page 275).

Referring to claims 10, 19, Rogaway discloses that the L and R values are elements of the offset factor Z (page 5), which meets the limitaiton of the second and fifth values are elements of a vector.

Referring to claim 14, Rogaway discloses that to compute the R value, the nonce is XOR'd with L and the result of the XOR function is encrypted with key K (Page 5), which meets

the limitation of the first and fourth values derived from the nonce value are permutations of a binary value computed by encrypting the nonce value using the block cipher and the first key.

Referring to claims 15, 16, Rogaway discloses encrypting a message by exclusive or'ing a block of the message with a corresponding block of a generated value (Page 5, $M[i] \oplus Z[i]$), which meets the limitation of whitening at least one message block with a third mask value. The result of that exclusive or operation is encrypted (Page 5) using a block cipher (Page 4), which meets the limitation of encrypting the at least one whitened message block using a block cipher and a first key. The result of the encryption is the exclusive or'ed with a corresponding block of the generated value (Page 5), which meets the limitation of whitening the at least one encrypted message block with the third mask value to generate at least one corresponding output ciphertext block.

Referring to claim 17, Rogaway discloses that the corresponding block of the generated value is generated based on the XOR of an encrypted nonce (Page 5, R) and an encrypted value (Page 5, L), which meets the limitaiton of the first and second mask values are computed by applying a XOR function to a first value derived from a nonce value and a second value derived from encrypting a third value using the block cipher and a key. Rogaway does not specify that the key used to encrypt the value to generate the 'L' (Page 5) is different than the key used to encrypt $M[i] \oplus Z[i]$ (Page 5). However, it would have been obvious to one of ordinary skill in the art at the time the invention was made to use multiple keys in the encryption algorithm in order to enhance the strength of the encryption algorithm by making the algorithm more difficult to break. Using only a single encryption key is easier break than using mutliple because an attacker would only need to discover the one key as opposed to having to discover every key that

Art Unit: 2132

is used in the encryption algorithm. Rogaway also does not disclose applying a substitution function to the result of the XOR function on L and R. However, it would have been obvious to one of ordinary skill in the art at the time the invention was made to perform a substitution function on the result of the XOR function on L and R because substitution operations are an important part of block cipher algorithms that give them security as taught by Schneier (Page 275).

Referring to claim 18, Rogaway discloses that the block cipher used is the AES block cipher (Page 6, first paragraph), which meets the limitation of the block cipher is AES.

Conclusion

15. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Art Unit: 2132

16. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Benjamin E. Lanier whose telephone number is 571-272-3805. The examiner can normally be reached on M-Th 6:00am-4:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.



Benjamin E. Lanier